ISSN(Online) : 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 5, Issue 3, March 2016

Simulation Analysis of Rushing Attack in DSR Protocol in MANETs

Ramneet Chopra[1], Sarabjit Kaur[2]

P.G. Student, Department of Computer Science & Engineering, CT Institute of Technology and Research, Jalandhar, Punjab, India[1]

Assistant Professor, Department of Computer Science & Engineering, CT Institute of Technology and Research, Jalandhar, Punjab, India[2]

ABSTRACT: Ad-hoc networks are multi hop wireless networks capable of establishing dynamic link without any pre existing infrastructure and centralized management. Due to its dynamic topology, open medium and scalable characteristics, these networks are more vulnerable to security attacks. Securing MANETs from various advisories at different layers of protocol stack becomes a challenging task. One such attack is rushing attack. It is network layer attack which decreases the probability of finding optimal route to destination. It exploits route discovery phase that works on principle of duplicate suppression for communication and become part of active route. Any on-demand routing algorithm which uses duplicate suppression for establishing route is vulnerable to this attack.

KEYWORDS: MANET, DSR protocol, Rushing attack, DoS.

I. INTRODUCTION

Mobile ad-doc network is a collection of wireless nodes that are capable of movement. Nodes can communicate with each other without the need of any pre-deployed telecommunication infrastructures such as base-stations or access points. Hence, these networks are also called infrastructure-less networks. Limited bandwidth and battery power are major constraints of these networks. Major applications of MANETs are to establish communicating environment at battlefield, disaster situations where using pre-existing environment for communication is not feasible. These networks are also used as network extensions.

For communication in these multihop networks various routing approaches are available. These approaches can be categorized as *proactive*, *reactive* and *hybrid*. Proactive approach maintains routing information at every node in network using routing tables. It uses periodic advertisements for gathering up to date network information. This approach is not very useful in case of mobile networks as topology changes frequently and imposes high routing overhead for e.g. Destination-Sequenced Distance-Vector Routing (DSDV). Reactive routing approach works on-demand basis and more adaptable to frequent topology changes in network. Examples of reactive approach are Dynamic Source Routing (DSR), Ad hoc on demand Distance vector (AODV). Hybrid routing protocols combines both proactive and reactive approaches for example Zone Based routing (ZRP). Due to its lack of centralized management and it operates on the principle of distributed cooperation; ad-hoc networks are more vulnerable to security attacks. These attacks may target data or a node or whole network performance.

II. DYNAMIC SOURCE ROUTING PROTOCOL

Dynamic source routing (DSR) protocol uses source routing algorithm which avoids the need for up-to-date routing information in the intermediate nodes through which packets are forwarded [1]. It comprises of two major phases: Route discovery and Route maintenance.

ISSN(Online) : 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 5, Issue 3, March 2016

A. Route discovery

DSR works entirely on demand basis. When source node wants to send data to destination node, it first checks its own route cache for route to destination. If route exists in route cache then source sends data by appending route in route record in packet header otherwise source initiates a route discovery by broadcasting a non-propagating route request packet (RREQ). By doing so source also determines if destination is in direct communication range or just one hop away. After sending first route request it waits for some time, if route reply arrives the source sends data on discovered route otherwise source broadcasts a propagating route request in entire network. Every node first checks the destination address in packet header if the packet reaches intended destination, node sends unicast route reply on route traversed by request packet by reversing the route stored in route record. Otherwise node rebroadcasts the request packet after appending its address in route record and the process continues until RREQ reaches destination. To limit this broadcasting overhead, every node forwards first received RREQ packet only and discards later packets.

B. Route maintenance

While using source route if link between source and destination breaks due to dynamic topology or node failure or some other means, route maintenance detects the broken route and generates route error packet back to source. If another route is available in source route cache then route is diverted otherwise new route discovery is initiated by source.

DSR protocol also provides some additional features like caching overheard routing information, replying using cached routes, automatic route shortening, packet salvaging etc. due to which DSR easily adapts frequent topological changes and able to work on highly dynamic network.

III. SECURITY ATTACKS

Security attacks can be classified into various categories. Some classifications are: *Active* and *passive*. Active attacks alter basic operations of network. It attempts to alter routing operation or attracts packets destined to other nodes, for example black hole attack. Whereas passive attacks do not make any disturbance in network operations, attackers are just seeking for useful information by listening to traffic. Traffic analysis and monitoring are examples of passive attacks. Passive attacks are more difficult to detect. Another classification is *Internal* and *external* attacks. In internal attacks, nodes already part of network becomes misbehaving nodes whereas in external attacks, nodes which are not part of network tries to manipulate network operations. External attacks in MANETs are easy to attempt due to its scalable properties and lack of centralized management.

There are various attacks are possible in MANETs and can be classified on basis of protocol stack. This paper is only concerned with network layer attacks so other attacks are not considered. Network layer attacks can also be classified into control plane attacks and data plane attacks. Control plane attacks exploits route discovery and route maintenance phase of routing protocols where as data plane attacks affects data forwarding phase by dropping, modifying or reordering data packets.

A. Rushing attack

It is malicious network layer attack which can be effective denial of service against all on demand routing protocols [1]. Rushing attack increases the probability that the discovered route includes the attacker node by quickly forwarding the RREQ packet broadcasted by source node. As each node only considers the first received RREQ packet and ignores later arriving RREQ by considering them duplicate. Hence, attacker node got selected in route.

Consider Figure 1, node S and D is source and destination respectively. M is malicious node. S generates the RREQ packet destined to D. Node M quickly forwards route request by ignoring broadcast jitter or routing delay provided by routing protocol. As destination only processes first received RREQ packet and ignores later arriving legitimate RREQ packets by considering them duplicate and thus attacker becomes part of route. Any routing protocol which uses duplicate suppression for communication in network is vulnerable to any of the variant of rushing attack.

ISSN(Online) : 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 5, Issue 3, March 2016

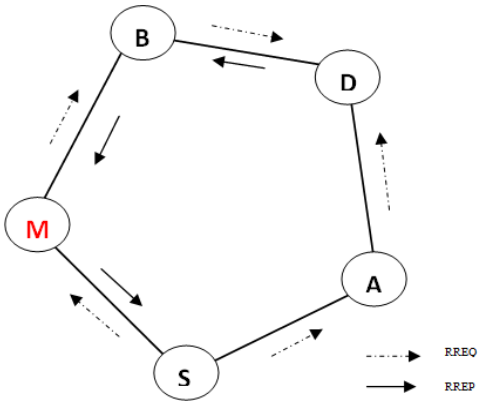

Figure 1. Rushing attack in network

B. Other variants of rushing attack

To quickly forward a RREQ packet so as to reach the destination earlier than other legitimate nodes, attacker may use any of the strategies mentioned in [1] as follows.

Ignoring routing/MAC delays: On-demand routing protocols delay RREQ forwarding so as to avoid collision of packets. Medium Access Control protocols generally add delay between when the packet is handed to the network interface for transmission and when the packet is actually transmitted. If the MAC layer does not specify a delay, on-demand protocols generally specify a delay between receiving a RREQ and forwarding it, in order to avoid collisions of the RREQ packets. Attacker may ignore either delay and thus becomes part of active route. Figure 1 can be considered as example topology of this variant.

Increasing transmission range: It is weakest strategy followed by attacker. Attacker increases its transmission range and reaches the destination by skipping nodes in between. Thus, pretends to the source as neighbor of destination and exploits data forwarding phase. Consider Figure 2, M is malicious node and sends RREQ packet received from source S by increasing its transmission range directly to neighbor of destination D. Thus skipping time consumed in hop by hop routing.

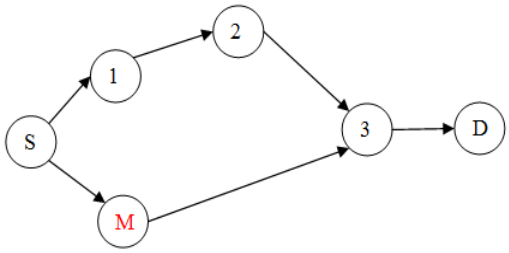

Figure 2: Example of rushing attack by increasing transmission range.

Inserting tunnel: It is strongest variant of the rushing attack. Attacker works in pairs and creates tunnel in the network. Consider figure 3, M and N are malicious nodes. Node M receives every RREQ and rather than broadcasting, it quickly forwards it to another malicious node N positioned near it. This makes sure every node near destination receive the RREQ packet forwarded by attacker node N. Hence attackers become the part the route.

ISSN(Online) : 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 5, Issue 3, March 2016

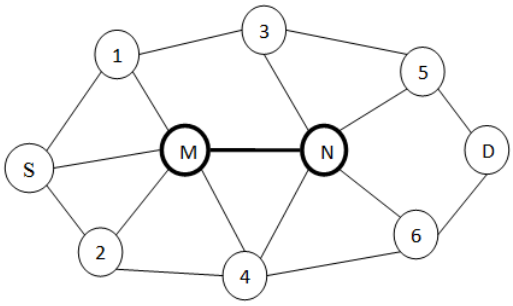

Figure 3: Example of rushing attack by inserting tunnel

C. Rushing attack as denial of service

In rushing attack, attacker exploits the route discovery phase to become part of route. Thus, it increases the chances of exploiting data forwarding phase. After got selected in route, attacker may impact network as following.

Route maintenance- Attacker node may drop route error packets during route maintenance phase in case of link breakage and make source unaware of link breakage which is more sever in case of highly dynamic networks.

Data forwarding phase- During data forwarding phase attacker node may drop packets resulting in black hole in the network or may reorder the data packets before forwarding them causing jellyfish attack which is severe in case of TCP based MANETs.

IV. SIMULATION MODELING

A. Metrics

Throughput- Throughput is measure of total number of bits transferred per second. It is computed in terms of Kbps (Kilo bits per second).

Packet delivery ratio- It is ratio of total number of packets received to total number of packet send.

End-to-end delay- It is measure of average time consumed by a packet to reach the destination and is computed in terms of ms (milliseconds).

B. Simulation modelling

For simulation study, Network Simulator 2 (version 2.35) is used [2]. For performance analyses AWK scripts are used [3]. There are several models present in the NS2 for wireless simulation. TABLE I shows the models used in the simulations. Reference [4] is used for MANET simulation study. To define mobility of wireless nodes random way point mobility model present already in NS2 is used.

TABLE I. SIMULATION MODELS

Model	Model name
Propagation model	Two ray ground
Mac type	802.11
Mobility model	Random way point
Traffic model	CBR/UDP

C. Attack model

In this study, attacker nodes are configured as malicious by creating tunnel in network. Therefore, probability of attacker node being selected in route increases. After got selected in the active route attacker node drops some data packets. We also tried to place attacker nodes near source so as increases the chances of attacker to be selected in route increases. For example topology of network, consider figure 3.

D. Simulation methodology

Simulation methodology is similar as in [5]. The goal of this work is to analyze the impact of rushing attack on network. So every simulation is first compiled with normal parameters and then same parameters are recompiled with rushing attack. Every simulation accepts scenario file which describes exact motion of nodes using mobility model as mentioned in TABLE I. To evaluate performance of particular factor, ten random simulation runs by giving 10 random scenario patterns as input are considered and performance of each considered factor is average of these ten simulation

ISSN(Online) : 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 5, Issue 3, March 2016

outputs. Simulation analysis is only concerned with metrics mentioned earlier in Section IV to analyze impact of rushing attack on network. So rest of metrics are not considered in this study.

V. EXPERIMENTS AND RESULTS

A. Design of experiments

Design of experiments are similar as in [6]. Two sets of experiments are created so far. General simulation parameters which are kept same in all experiments are mentioned in Table II. Reference [7] is used for DSR protocol configuration parameter values. Moving speed of wireless node is randomly chosen by node between zero and maximum mobility speed.

TABLE II. SIMULATION PARAMETERS

Parameter	Value
Simulation area(meters)	1000*1000
Simulation time(sec)	250
Packet size(bytes)	512
Number of packets per second	20
Transmission range(meters)	250
Bandwidth(Mbps)	2
Pause time(sec)	1
Number of attacker nodes	4

Experiment 1: Varying number of network nodes.

Number of nodes in network is varied from 50 to 100 incremented by 10. Maximum speed of nodes is 2.5 m/sec. For results of this experiment, refer Figure 2, 3, 4.

Experiment 2: Varying mobility speed of mobile nodes.

Velocity of wireless nodes are varied from zero mobility i.e. static to highest mobility speed i.e. 10 m/sec and increased by factor 2.5. Pause time is 1 sec. Mobility model is same as mention in TABLE I. Number of nodes are 100. And number of attacker nodes are 4. Rest of the parameters remains same as mention in TABLE I and TABLE II. For results of this experiment, refer Figure 5, 6, 7.

B. Results

Figure 4, 5, 6 shows impact of rushing attack decrease with increases in network nodes. It is known by fact that as the node density increases, neighbor count also increases which decreases the chances of rusher node to be selected in route. Hence, the maximum mobility in this experiment is only 2.5 m/sec which shows that the average number of link failures is significant factor for metrics loss. Results show least performance loss in case of 100 nodes as it shows minimum impact. This significant difference is also due to the fact of random deployment of nodes.

Figure 7, 8, 9 shows that impact of rushing attack increases with increase in mobility speed of mobile nodes. This is due to fact that with increase in velocity of mobile nodes average number of link changes increases due to dynamic topology and it is also a considerable reason of decreasing network performance. As the network is in promiscuous mode which increases the chances of fact that nodes are more aware of changing topology and are able to capture control information and learn the routing information due to DSR protocol route cache technology. Due to this fact, packet delivery ratio and throughput does not show major loss in case of normal DSR but in case of rushing attack in both experiments, results shows significant loss.

ISSN(Online) : 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 5, Issue 3, March 2016

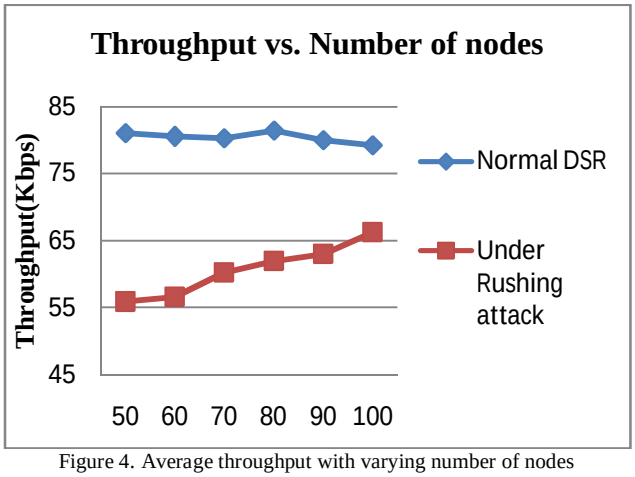

Figure 4. Average throughput with varying number of nodes

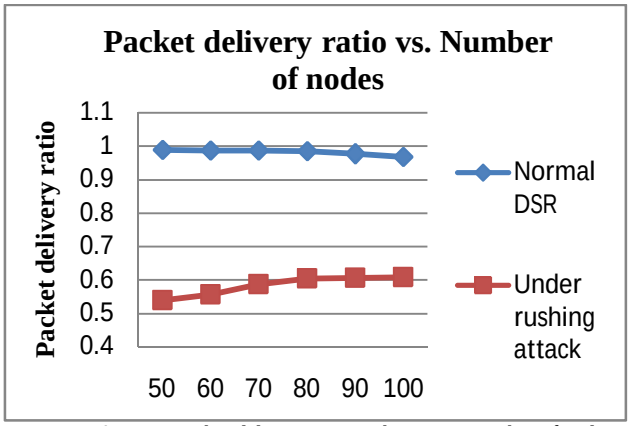

Figure 5. Average packet delivery ratio with varying number of nodes

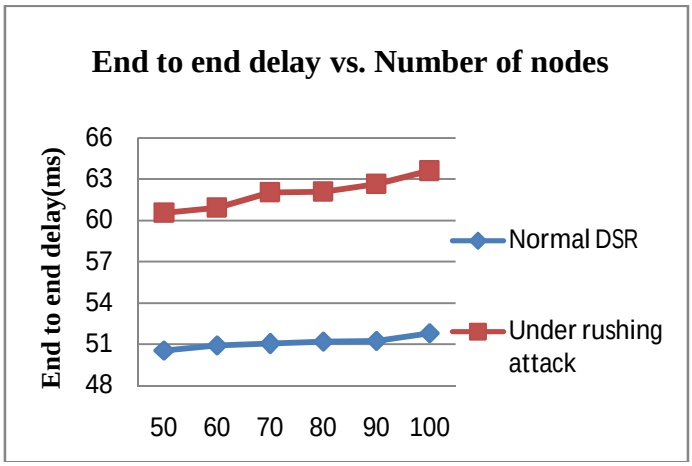

Figure 6. Average end to end delay with varying number of nodes

ISSN(Online) : 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 5, Issue 3, March 2016

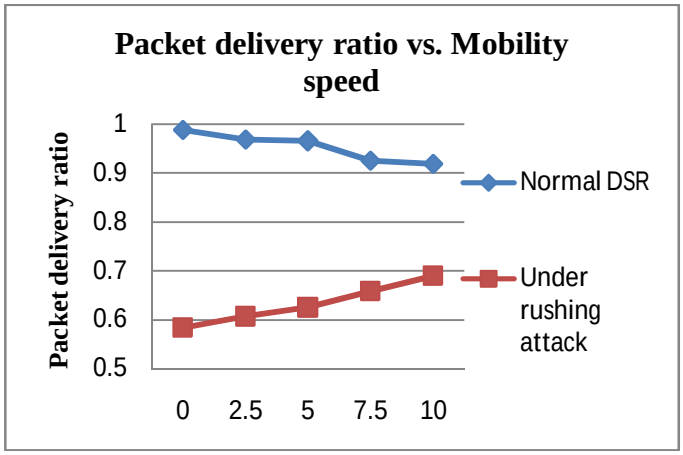

Figure 7. Packet delivery ratio with varying mobility

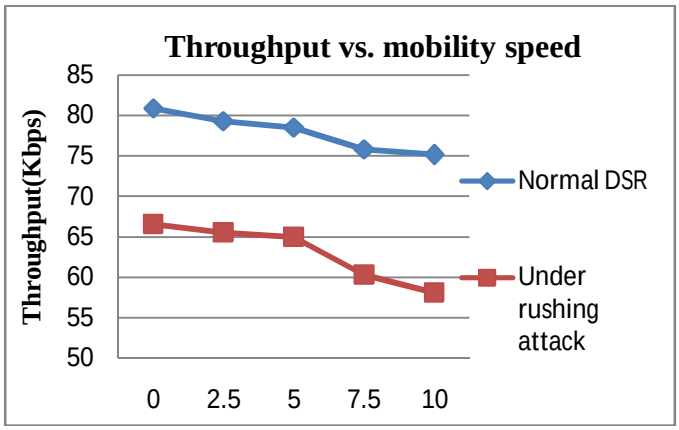

Figure 8. Throughput with varying mobility

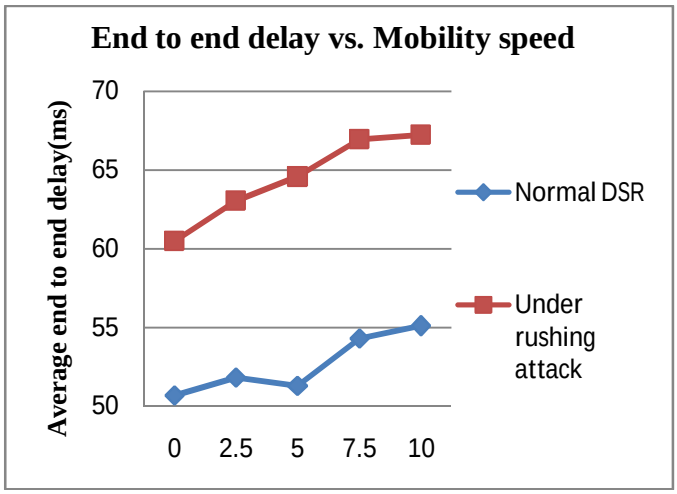

Figure 9: Average end to end delay with varying mobility

ISSN(Online) : 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 5, Issue 3, March 2016

VI. CONCLUSION

With this experimental study, it is observed that when source and destination is in direct communication range impact of rushing attack goes to zero. It is lowest when node density is highest. Mobility factor is also significant in network performance. It is observed from simulations that when attacker is near to source and destination chances of successful attack increases. Chances of attacker to be selected in the active route also depend upon distance of attacker from source and destination.

With the increase in node density impact of attack minimize. It is also observed in the simulations that if more than one attacker positioned consecutively in the network then it also prevents the discovery of shorter routes available in the network. Due to which source may not able to detect optimal routes. This situation becomes severe in case of high mobility as dynamic topology increases the control overhead and thus effect the throughput and packet delivery ratio.

FUTURE SCOPE

Further study may include analysis of routing overhead imposed by routing protocol and energy consumption. Impact of rushing attack could be compared in case of AODV and other on demand routing protocols.

REFERENCES

[1] Y.-C. Hu, A. Perrig, and D. B. Johnson, “Rushing Attacks and Defense in Wireless Ad Hoc Network Routing Protocols,” *Proc. 2003 ACM Work. Wirel. Secur. (WiSe ’03)*, pp. 30–40, 2003.

[2] K. Fall and K. Varadhan, “The ns Manual (formerly ns Notes and Documentation),” *VINT Proj.*, no. 3, p. 434, 2011.

[3] A. D. Robbins, *GNU Awk*. 2014.

[4] S. Kurkowski, T. Camp, and M. Colagrosso, “MANET simulation studies: the incredibles,” *ACM SIGMOBILE Mob. Comput. Commun. Rev.*, vol. 9, no. 4, pp. 50–61, 2005.

[5] S. Mohapatra and P. Kanungo, “Performance analysis of AODV, DSR, OLSR and DSDV Routing Protocols using NS2 Simulator,” *Procedia Eng.*, vol. 30, pp. 69–76, 2012.

[6] P. Johansson, T. Larsson, N. Hedman, B. Mielczarek, and M. Degermark, “Scenario-based performance analysis of routing protocols for mobile ad-hoc networks,” *5th Annu. ACM/IEEE Int. Conf.*, pp. 195–206, 1999.

[7] D. Johnson, Y. Hu, and D. Maltz, "The Dynamic Source Routing Protocol (DSR) for Mobile Ad Hoc Networks for IPv4", RFC 4728, DOI 10.17487/RFC4728, February 2007.

.